Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996:	)	
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information	)	CC Docket 96-115

COMMENTS OF NEW AMERICA FOUNDATION'S OPEN TECHNOLOGY INSTITUTE, BENTON FOUNDATION, CENTER FOR MEDIA JUSTICE, CHICAGO MEDIA ACTION, FREE PRESS, INSTITUTE FOR LOCAL SELF-RELIANCE, MEDIA ALLIANCE, PEOPLES PRODUCTION HOUSE, PUBLIC KNOWLEDGE, AND THE PEOPLES CHANNEL & DURHAM COMMUNITY MEDIA

Sarah J. Morris
Benjamin Lennett
Open Technology Institute
New America Foundation
1899 L Street, NW, 4th Floor
Washington, DC 20036

July 13, 2012

TABLE OF CONTENTS

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Implementation of the Telecommunications Act of 1996:	)	
	)	
Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information	)	CC Docket 96-115

COMMENTS OF NEW AMERICA FOUNDATION'S OPEN TECHNOLOGY INSTITUTE, BENTON FOUNDATION, CENTER FOR MEDIA JUSTICE, CHICAGO MEDIA ACTION, FREE PRESS, INSTITUTE FOR LOCAL SELF-RELIANCE, MEDIA ALLIANCE, PEOPLES PRODUCTION HOUSE, PUBLIC KNOWLEDGE, AND THE PEOPLES CHANNEL & DURHAM COMMUNITY MEDIA

New America Foundation's Open Technology Institute, Benton Foundation[1], Center for Media Justice, Chicago Media Action, Free Press, Institute for Local Self-Reliance, Media Alliance, Peoples Production House, Public Knowledge, and The Peoples Channel & Durham Community Media (together, "Commenters"), respectfully submit these comments in response to the *Public Notice* ("PN") released by the Federal Communications Commission's Wireline Competition Bureau, Wireless Telecommunications Bureau, and Office of General Counsel in the above-captioned docket. The PN seeks comments "regarding the privacy and data-security practices of mobile wireless service providers with respect to customer information stored on

[1] The Benton Foundation is a nonprofit organization dedicated to promoting communication in the public interest. These comments [or this press release] reflect the institutional view of the Foundation and, unless obvious from the text, are not intended to reflect the views of individual Foundation officers, directors, or advisors.

their users' mobile communications devices, and the application of existing privacy and security requirements to that information."[2]

SUMMARY

As the Commission correctly notes in its Public Notice, it is time to refresh the record "concerning the practices of mobile wireless service providers with respect to information stored on their customers' mobile communications devices."[3] New America Foundation's Open Technology Institute, Benton Foundation[4], Center for Media Justice, Chicago Media Action, Free Press, Institute for Local Self-Reliance, Media Alliance, Peoples Production House, Public Knowledge, and The Peoples Channel & Durham Community Media that in so doing, the Commission should carefully examine the data collection practices of carriers as well as those of the applications, like Carrier IQ, under the carriers' direction.

Commenters ask the Commission to find that these data collection practices fall within the scope of CPNI contemplated in § 222 of the Telecommunications Act and do not clearly fall under any of the statutory exemptions listed in the statute. Importantly, Commenters highlight the need for the Commission to not merely take the carriers' self-assessments of these practices at face value, given the variety of incentives in play as well as the carriers' inconsistencies in the 2007 proceeding.

In addition, Commenters ask the Commission to adopt an "opt-in" rather than "opt-out" disclosure and consent regime for all collection by carriers and applications under their direction

---

[2] *Privacy and Security of Information Stored on Mobile Devices*, Public Notice, CC Docket No. 96-115 (rel. May 25, 2012) at 1.

[3] *Id.* at 4.

[4] The Benton Foundation is a nonprofit organization dedicated to promoting communication in the public interest. These comments [or this press release] reflect the institutional view of the Foundation and, unless obvious from the text, are not intended to reflect the views of individual Foundation officers, directors, or advisors.

of CPNI data as well as any sharing of CPNI data to third parties. Given the degree to which applications like Carrier IQ are integrated into mobile device architecture, it is extremely difficult for ordinary users to both understand how those applications are being used, and also to know how and when to take adequate safeguards to protect their personal data.

Finally, Commenters ask the Commission to require carriers to re-disclose their data collection and sharing practices and renew customer consent once every six months. This requirement reflects the rapid pace at which mobile technology evolves and allows customers the opportunity to reflect on whether the collection of CPNI data aligns with their current privacy values. In addition, the requirement keeps the issue of privacy protection present both for individuals and for the group of mobile device customers as a whole, increasing broadly the level of engagement and understanding of privacy concerns in this space.

I. INTRODUCTION

Questions related to mobile privacy have been present in every recent discussion of privacy in the digital age. While Commenters recognize the importance of privacy in a multitude of contexts, the issue presented by the Commission represents one of notable urgency given the special relationship between mobile service providers and consumers, the sensitivity of the data being collected by those service providers, and the highly concentrated nature of the mobile service market. Providers have every incentive to continue to collect CPNI data about their customers, either directly or through services like Carrier IQ, and consumers are presently disadvantaged in their ability to protect the privacy of their personal data stored on their mobile devices.

Commenters therefore urge the Commission to recognize current collection practices as a violation of the duty outlined in § 222 of the Telecommunications Act. Commenters also ask the Commission to impose requirements on mobile service providers to disclose their current data collection practices to consumers, including what data is being collected, for what purposes that data is being used, and to what additional parties that data is being disclosed, and to obtain explicit opt-in consent from consumers to so use that data. Finally, Commenters ask the Commission to impose also a requirement that carriers must re-disclose and renew a consumer's opt-in consent to those practices once every six months following the initial consent.

II. DIRECTING APPLICATIONS TO COLLECT AND/OR TRANSMIT CPNI DATA IS IN VIOLATION OF § 222.

Carriers can no longer hide behind their assertions in the Commission's 2007 proceeding, in which they abdicated any responsibility for information stored on mobile devices. Technology has evolved and now allows carriers to collect, either themselves or via third-party applications

like Carrier IQ, consumer data at an extremely granular level and of an extremely personal nature. The Commission must now recognize that this activity falls within the type protected as CPNI under § 222 and that mobile service providers' expressed use of the collected data does not fall under any statutory exemptions.

a. Data stored on mobile devices is CPNI.

CPNI is defined as "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."[5] As the Commission notes, CPNI includes information such as the phone numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting."[6]

Much of the data stored on mobile devices is precisely the type of data contemplated by the statute in section (A), and also section (B), as in many instances where carriers provide detailed call, text, and data logs to consumers through their web pages.[7] Sprint stated in 2007, without justification or further explanation, that "none of the information generated by the customer and stored in the handset is CPNI because (a) it is not available to the carrier by virtue

[5] 47 U.S.C. § 222(h)(1).

[6] *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007) ("2007 Order") ¶ 5.

[7] Texting and data logs would also fall under (B), not simply because they are listed on a cell phone bill, but also because they pertain to a telecom service insofar as (1) texting and data are part of the same billing package as voice, used on the same device, advertised and marketed as part of the same service, and (2) they use the consumer's phone number.

of the carrier/customer relationship; (b) the information is not in possession of the carrier; and (c) with the exception of an abbreviated call-history list which the customer may delete, none of the information relates to the 'quantity, technical configuration, type, destination, location and amount of use' of the subscribed telecommunications service. Nor does it constitute information that carriers include in their bills to customers."

Regardless of whether or not this blithe assertion was accurate in 2007,[8] it can no longer pass muster given even the most generous assessment of the current cellular landscape. Even basic "feature phones" contain detailed (one would hardly call them "abbreviated") call logs that include not just who the user was calling but also the frequency, duration, and timing of such calls. The phones also store similar information about texts, picture texts, and video texts. Smart phones store all of that information and more.[9] This data is prototypical of the type of data that the Commission has explicitly considered to be CPNI, and carriers admit to using software like Carrier IQ to pull such information from users' cellular devices.[10]

All of this information is also within the possession of the carrier, whether it is accessed directly by the carrier from the customers' phones or through an application like Carrier IQ. Without even looking to the technical architecture and capabilities of the phones and applications

[8] Indeed, Commenters note (here and in section II (b), below) that it was almost certainly not true, by Sprint's own admission. *See*, Letter from Vonya B. McCann, Senior Vice President, Government Affairs, Sprint Nextel, to The Honorable Al Franken, United States Senate (Dec. 14, 2011) ("Sprint Letter to Sen. Franken") at 2, where Sprint notes it "began including Carrier IQ software devices in 2006," a date that is clearly prior to the company's 2007 comments.

[9] Sprint notes specifically that, using Carrier IQ, it collects, for example, the URLs of websites that its customers visit. Sprint Letter to Sen. Franken at 3.

[10] Letter from Timothy P. McKone, Executive Vice President, Federal Relations, AT&T Services, Inc., to The Honorable Al Franken, United States Senate (Dec. 14, 2011) ("AT&T Letter to Sen. Franken"): "To improve customer service, the CIQ software provides AT&T with the location, date and time the handset experiences a network event, such as a dialed or received telephone call, a dropped call or an attempted call when the handset has no signal. This information tells AT&T where the device was at the time of the occurrence …."

pre-installed by carriers, it is easy to see the direct connection between the data stored on the phones and the data provided to consumers through either a paper copy of their monthly bill or ongoing access to that same information via password-protected access to the carrier's website.

For this reason, the data also fits within definition (B), which classifies as CPNI "information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier." Providing this information to customers as part of their monthly bill or online account indicates that it is both in the carriers' possession and also CPNI by this alternative statutory definition.

Finally, this data is also "made available to a carrier by the customer solely by virtue of the carrier-customer relationship." To hold otherwise would be contrary to the carriers' own acknowledgement that they use this data specifically "to improve customer service"[11] and their explanation as to how the data is collected, stored on mobile devices, and then transmitted to carriers' servers for the purpose of evaluating network performance. Carriers admit to using Carrier IQ to collect this data, and that collection is clearly by virtue of the carrier-customer relationship – carriers would not have access to the data (or need for it at all, according to their explanation) but for their relationship with their customers.

b. Carrier use of information stored on mobile devices does not fall under the statutorily permitted uses within § 222(c), (d), or (f).

Section 222(c)(1) provides that a carrier may only use, disclose, or permit access to customers' CPNI in limited circumstances. For example, § 222(c)(1) permits a telecommunications carrier to do so "in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications serve, including the publishing of directories." Section 222(d) provides

[11] AT&T Letter to Sen. Franken at 2.

exceptions when carriers are billing consumers; providing inbound (customer-initiated) telemarketing, referral or administrative services; or providing call location information in the case of emergencies. Section 222(f) also provides that for the purposes of § 222(c)(1), without the "express prior authorization" of the customer, a customer shall not be considered to have approved the use or disclosure of or access to (1) call location concerning the user of a commercial mobile service or (2) automatic crash notification to any person other than for the use in the operation of an automatic crash notification system.

Based on the responses contained in letters to Senator Franken from a limited number of carriers, it appears that some carriers arguments may rely on § 222(c)(3), as they emphasize that they use the Carrier IQ software to collect data for "network and service improvement purposes."[12] However, more detailed information in the Commission's record is needed to evaluate this potential justification, as carriers have an incentive to collect the (very valuable) CPNI data for a variety of purposes beyond network and service improvement. Moreover, they have a history of not being forthcoming with information about how and why they are collecting data, and for what purposes they are using it.

The Commission cannot simply take at face value the carriers' assertion that they need and use customer data collected by Carrier IQ solely for the provisioning of telecommunications service. The reason that CPNI data is given strong, explicit statutory protections under the Telecommunications Act is due to the value and sensitivity of the data. Indeed, the data collected by Carrier IQ would be extremely valuable to both carriers and other entities. The Internet

[12] *Id*. *See also* Sprint Letter to Sen. Franken at 1, which notes that "[t]o help [Sprint] better understand these issues, Sprint uses troubleshooting software installed on customers' devices to report diagnostic and analytics data so it can solve particular problems."

advertising market is the U.S. is worth an estimated $300 billion,[13] and the data collection available to carriers through applications like Carrier IQ would provide them with a treasure trove of consumer data to sell targeted ad space and in-depth market research on their customers. Moreover, as carriers become involved in offering additional services such as mobile money, they have the ability to combine multiple categories of personal information, such as financial information, with other information collected by applications like Carrier IQ to develop comprehensive profiles of their customers. With the growing market for personal information—and the increasing number of sharing and direct acquisitions of consumer data – it is impossible for consumers to know with whom one's data will end up and with what other information it may be combined. Given the market's demand for personal data, in the long run it is almost inevitable that this information will be combined and mined in ways the user never imagined or consented to.

Carriers not only have the incentive to collect CPNI data for purposes other than improved delivery of communications services; they also have proven historically unreliable in their disclosure of how and for what purpose they collect the data. For example, Sprint indicated in its 2007 comments that "[w]ireless carriers are not well-positioned to guarantee the privacy of customer information stored on devices" because those devices are "in the physical control and custody of customers."[14] However, in its 2011 letter to Senator Franken, the company revealed it had been installing Carrier IQ on devices since 2006.[15] At the time it submitted the 2007 comments, Sprint would therefore clearly have been aware of its own increasing ability to access

[13] *See* Economic Value of the Advertising-Supported Internet Ecosystem, iab.net (June 10, 2009) *available at* http://www.iab.net/insights_research/industry_data_and_landscape/economicvalue.

[14] Comments of Sprint Nextel Corporation, CC Docket No. 96-115 and WC Docket no. 04-36, (July 9, 2007) ("Sprint 2007 Comments") at 21.

[15] Sprint Letter to Sen. Franken at 2.

data stored on mobile devices, even if it had not yet begun collecting that data widely. This contradiction indicates an unwillingness of carriers, who are actually the *best*-positioned to know about their own capabilities to access customer data stored on mobile devices, to be forthcoming about such capabilities.

In addition, Carrier IQ has the ability to collect a wide range of data, not all of which is related to delivery of service. Not every *possible* data-collection ability is one that should conversely be deemed *permissible*. For example, it is problematic for applications like Carrier IQ to log the URLs of the sites a user visits, especially when that user is browsing using HTTPS, as many secure URLs contain the username and password of the client user.[16] Storing this information in the devices' (and potentially, the carriers') logs represents an unnecessary risk to the user and is a serious privacy breach, particularly in light of the fact that by using a secure connection, the user has most certainly demonstrated an intention to protect his or her privacy.[17]

In addition, by carriers' own admission, applications like Carrier IQ also log time stamps for when SMS messages are sent and received.[18] While this information may be useful for evaluating network performance, observers note that the software can also be used to log the contents of these messages.[19] Similar to the collection of full URLs, there is no clear reason why the contents of the text messages would affect performance, and this collection activity similarly

---

[16] *See* Trevor Eckhart, Carrier IQ, Android Security Test, *available at* http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/ and http://androidsecuritytest.com/features/logs-and-services/loggers/carrieriq/carrieriq-part2/ ("Eckhart Carrier IQ")

[17] Indeed, more to the point below, this action alone should be interpreted as clearly "opting out" of data collection.

[18] *See e.g.* AT&T Letter to Sen. Franken at 2-3.

[19] *See* Eckhart Carrier IQ; *see also* Letter of the Honorable Al Franken, United States Senator to Mr. Larry Lenhart, President, Carrier IQ, Inc. (November 30, 2011) ("Sen. Franken Letter").

represents an unnecessary risk that applications like Carrier IQ, and the carriers that use them, are taking on behalf of their (unsuspecting) users.

Thus, before the Commission can even consider whether the carriers' use of Carrier IQ to falls within the bounds contemplated by § 222(c)(3), a much more robust record must first be established, with the carriers' assertions (made in their own interest) about the scope of actual and potential collection of data verified by independent, trustworthy sources.[20] Without additional transparency or independent evaluation, it remains unclear what data is actually being collected and for what purposes. Currently available information suggests cause for great concern, as Carrier IQ and related applications are designed to be able to harvest a great deal of user information, some of which simply has no utility for network performance, and much of which has significant financial or market value to the entities collecting the data.

III. CURRENT DISCLOSURE AND CONSENT REQUIREMENTS ARE INADEQUATE TO ENABLE CONSUMERS TO MAKE MEANINGFUL DECISIONS ABOUT THEIR PRIVATE DATA.

Given the uncertainties surrounding the type of data collected by carriers, how it is used, and with whom it is shared, combined with the level of sensitivity of the data that is being collected, the Commission should impose an opt-in consent requirement on carriers for data stored on mobile devices and collected either directly by carriers or at the direction of carriers using a third-party application like Carrier IQ. Further, the Commission should require that carriers revisit and renew that consent every six months following the original consent in order to

[20] Senator Franken has also highlighted his doubts about the trustworthiness of the carriers' disclosure and the relationship of Carrier IQ's use to service provision: "I understand the need to provide usage and diagnostic information to carriers. I also understand that carriers can modify Carrier IQ's software. But it appears that Carrier IQ's software captures a broad swath of extremely sensitive information from users that would appear to have nothing to do with diagnostics – including who they are calling, the *contents* of the texts they are receiving, the *contents* of their searches, and the websites they visit." [emphasis in original], Sen. Franken Letter at 1.

give users the opportunity to change their consent status as users' privacy concerns and need evolve.

a. Protection of CPNI data necessitates heightened privacy protections whether or not the carriers are collecting the data themselves or directing a third-party application to collect the data, and Commenters therefore request that the Commission apply an opt-in, rather than opt-out, requirement to protect CPNI data.

Given the way applications like Carrier IQ are designed and utilized, the fundamental question of whether it is even possible for users opt out of having their data collected remains. Carrier IQ comes pre-installed on mobile devices at such a deep level within the device's architecture that it is almost entirely hidden from the user. It runs from the boot file on the smartphone, it cannot be halted, and removing it requires a degree of technical sophistication that it is unreasonable to expect of ordinary users (most of whom are unaware of its very existence). Thus, an opt-out system in which a company that collects or shares data "must give consumers an opportunity to deny them permission to do so, or opt out"[21], does not work in this context because users do not have the opportunity to learn that their information is being collected (by virtue of the application's design) and therefore do not have any meaningful opportunity to decline consent. With that concern in mind, an opt-in requirement, where companies have "to obtain a consumer's explicit consent before [collecting or] sharing personal information about them"[22] is the minimum level of protection that could be sufficient to allow for informed consent.

The Telecommunications Act and past Commission rulemakings also provide support for an opt-in consent requirement specifically in instances where data is shared with third parties.

[21] Jan Bouckaert and Hans Degryse, Opt In Versus Opt Out: A Free-Entry Analysis of Privacy Policies, CESIFO Working Paper No. 1831 (October 2006) at 3 [*citing* J. Lacker, The economics of financial privacy: To opt out or opt in?, *Economic Quarterly*, 88].

[22] *Id.*

Section 222 provides different levels of protection for the varying degrees of data sensitivity. In particular, the statute acknowledges the particular sensitivity of CPNI. As the Commission has noted, "Congress accorded CPNI, the category of customer information…the greatest level of protection under this [statutory] framework."[23] The Commission is tasked with ensuring that carriers are protecting this data adequately, and the Commission therefore "has a substantial interest in protecting customer privacy."[24]

To that end, the Commission has found that "there is a substantial need to limit the sharing of CPNI with others outside a customer's carrier to protect a customer's privacy. The black market for CPNI has grown exponentially with an increased market value placed on obtaining this data…"[25] The Commission therefore took specific, additional regulatory steps in 2007 to ensure that carriers adequately guarded against third-party threats such as pretexting. These steps included password verification before releasing consumer data and other "reasonable steps" such as encryption of CPNI databases.[26]

In addition, the Commission modified the disclosure requirement when CPNI is disclosed to telecommunications carriers' joint venture partners and independent contractors, shifting from an opt-out to opt-in requirement. The Commission notes that "current opt-out notices allowing carriers to share information with joint venture partners and independent contractors are often vague and not comprehensible to an average customer," finding therefore that "simply modifying our existing opt-out notice requirements will not alleviate these concerns because opt-out notices do not involve a customer actually authorizing the sharing of CPNI in the first instance, but

[23] 2007 Order ¶4.

[24] 2007 Order ¶37.

[25] 2007 Order ¶39.

[26] 2007 Order ¶36.

rather leave it to the carrier to decide whether to share it after sending a notice to the customer, which the customer may or may not have read."[27]

While the use of the Carrier IQ software to collect data stored on mobile device differs somewhat from the scenario noted above, where a customer's CPNI is sent by the carrier to a third-party vendor for marketing purposes, the situation is nonetheless sufficiently analogous that a similar rule is warranted for both the collection of CPNI data directly or by third parties and any subsequent sharing of that data. The fact that Carrier IQ is merely operating under the direction of the carriers is irrelevant, as the concerns the Commission noted in the 2007 Order hold here as well, and there is no guarantee that Carrier IQ is taking or will take adequate safeguards to protect the data it is entrusted by the carriers to collect. In addition, while carriers may be able to speak to the data security practices embedded in their own corporations, they cannot speak with authority to the practices of Carrier IQ or whatever other third-party they may employ to collect the data in the future.

Finally, other research confirms that opt-out requirements are simply insufficient for protecting user privacy. As EPIC noted in its Amicus Brief in support of the aforementioned Commission rule, an "opt-out approach is inadequate because it is not calculated to reasonably inform consumers about their privacy options, and often customers may not know that they must affirmatively act…"[28] In addition, opt-out requirements add additional transaction costs. "Opt-

[27] 2007 Order ¶40.

[28] Brief for Privacy and Consumer Organizations, Technical Experts and Legal Scholars as *Amici Curaie* in Support of Respondents Urging the Court to Deny the Petition for Review of the FCC's 2007 Order, National Cable & Telecommunications Association v. Federal Communications Commission and United States of America, United Sates Court of Appeals, District of Columbia (May 6, 2008) ("EPIC Amicus") at 8.

out regimes create an economic incentive for businesses to make it difficult for consumers to exercise their preference not to disclose personal information to others."[29]

Thus, the average user has little experience navigating the complexities of privacy in the digital age, and cannot be expected to fully understand the implications of how their data is being collected, let alone with whom the carriers or applications like Carrier IQ are sharing their data. In order for a consent regime to be effective, carriers must be required to disclose what data they are collecting, what mechanisms and applications they are using to collect that data, and with whom they are sharing that data. In return, users must give explicit opt-in consent that indicates that they have read and understand those policies.

b. Commenters also request a requirement that carriers resubmit the opt-in request to customers once every six months and re-solicit consent from those customers to continue collecting customer data directly or using Carrier IQ or other applications.

Finally, Commenters ask the Commission to additionally require companies to "re-up" the consent they receive from customers after a discrete period of time. Commenters suggest a six-month period to account for the frequently rapid shifts in the market and carrier needs, and also to reflect changing needs and desires of the users.

Users' privacy concerns fluctuate over a lifetime of mobile device use, and their "privacy calculus" may change dramatically at any point, for any number of reasons. In addition, mobile device users must respond to dozens (or even hundreds, depending on how many "apps" they use) of requests for consent to access various amounts of data on their machines over the life of the phone. One request, even if it is an opt-in request, from a carrier to gather data using third-party applications will likely get lost in this shuffle. Given the highly-sensitive nature of CPNI

[29] *Id.* at 9 (citing Jeff Sovern, *Toward a New Model of Consumer Protection: The Problem of Inflated Transaction Costs*, 47 Wm & Mary L. Rev. 1635, 1624 (2006)).

data as explained above, a step beyond the requirement set for third-party disclosure in 2007 is now needed.

Thus, Commenters recommend that the Commission require carriers to re-disclose how the user's CPNI data will be used and re-acquire opt-in consent from user once in each six-month period following the original opt-in consent. By revisiting the consent process, users have the ability to reflect on whether the collection of CPNI data aligns with their current privacy values, and keeps the issue of privacy protection in the front of users' minds, encouraging more deliberate privacy protection behavior at both the individual and societal level. The latter justification is important beyond just CPNI data and carrier behavior; more deliberate and informed behavior in one area of mobile data collection can lead to more awareness of privacy concerns in other areas as well.

IV. CONCLUSION

For the reasons outlined above, Commenters urge the Commission to recognize that carrier-directed collection of data falls within the purview of § 222, that the data collected is CPNI, and that it does not fall under one of the statutory exemptions. Given the Commission's responsibility to ensure that CPNI data is adequately protected by mobile service providers, Commenters request that the Commission impose an explicit, opt-in consent requirement on carriers to ensure that consumers understand what data is being collected, for what purposes it is being used, and with whom it is being shared. Further, Commenters request that the Commission impose a requirement that carriers re-disclose and renew customer consent once ever six months in order to account for rapid shifts in mobile technology and evolving privacy values among consumers.

Respectfully submitted,

/s/ Sarah J. Morris

Sarah J. Morris
Benjamin Lennett
Open Technology Institute
New America Foundation
1899 L Street NW, 4th Floor
Washington, DC 20036
(202) 986-2700
morriss@newamerica.net